# *Data-At-Rest (DAR)*

## *"Protection of PII and SI"*

**(**Please read all notes included with the slides**)**

Data-At-Rest is Data-At-Risk!

# Data-At-Rest (DAR) Training

- **PURPOSE: The purpose of this training is to provide you information on the new Data-At-Rest policy and program**
- **OBJECTIVES: At the end of this briefing, you will learn:**
  - **Why the DAR Program is important**
  - **Understand the DAR Policy**
  - **How to encrypt PII and SI by using the "Encrypt" Folder**
  - **What to do when preparing for travel**
  - **Requirements while traveling**
  - **What to do when returning from travel**

# Agenda

- Purpose
- History
- Definitions
- User Responsibilities
- How to Use the "Encrypt" Folder
- Why important
- Preparing for travel
- While traveling
- Returning from travel
- Protecting Personally Identifiable Information Video
- DAR Policy References

## Purpose

- **To increase awareness and educate users on the new policy requirements for Data-At-Rest, including the protection of Sensitive Information (SI) and Personally Identifiable Information (PII)**

- **Instruct users how to use the "Encrypt" Folder on the desktop**

# History

Los Angeles Times
latimes.com
American investigators have paid thousands of dollars to buy back the stolen drives, according to shopkeepers outside the major military base here..
.... By Paul Watson, Los Angeles Times | April 15, 2006

CORPS
MarineTimes.com
Lost laptop contains 2,400 Pendleton Marines' info
By John Hoellwarth
Staff writer
A laptop computer belonging to the civilian company that manages base housing at Camp Pendleton, Calif., has gone missing, and the personal information of about 2,400 Marines who live on base along with it, according to an Oct. 6 Marine Corps news release.

- **ALARMED by the new information security threats and the loss of PII and SI**
- **Army policy, standards, and guidance have existed since 2003 and relied on voluntary management enforcement**
- **Data-At-Rest is Data-At-Risk!**

## Definition

- **Personally Identifiable Information (PII)**
- **Sensitive Information (SI)**
- **Data-At-Rest (DAR) Devices**
  - **Mobile Computing Device (MCD)**

- **Data Storage Device (DSD) / Removable Media**
- **Government Facility**
- **The DAR Policy is punitive in nature IAW AR 25-2.**

# Responsibilities

**Users:**

- **Identify and maintain accountability for all government MCDs/DSDs in your possession**
- **Ensure all devices are properly marked**
- **Secure all devices from theft and pilferage**
- **Encrypt all sensitive data on devices in their possession**
- **Use the "Encrypt" Folder in your Documents Folder for encryption of all sensitive data**
- **Use only government approved/owned devices**
- **Complete the Common User Training CBT and sign the Acceptable Use Policy (AUP)**
- **Ensure system is scanned upon returning**
- **Report any loss of information**

# Using the "Encrypt" Folder

**Use the "Encrypt" Folder on your desktop to encrypt all sensitive data and Personally Identifiable Information (PII) by one of two options:**

1. **Copy all those files in the "Encrypt" Folder and then delete them from where you copied them, after you have verified that all those files are in that folder**

2. **Or you can drag and drop them into the "Encrypt" Folder**

** **Choose whatever option you are most comfortable with doing. If you are unsure of the instructions please contact your Unit or Garrison IA personnel****

# Why is This Important

Los Angeles Times
latimes.com

**American investigators have paid thousands of dollars to buy back the stolen drives, according to shopkeepers outside the major military base here..**

**…. By Paul Watson, Los Angeles Times | April 15, 2006**

MSNBC.com

Stolen military data for sale in Afghanistan

Despite crackdown, computer drives found with names of alleged spies

## Why is This Important

- ✓ **One flash memory drive, sold for $40, holds the *names, photos and phone numbers of people described as Afghan spies* working for the military. Other thumb drives have been found to contain:**
  - **…*Social Security numbers listed next to the names of hundreds of Soldiers***
  - **…*names of senior Afghan ministers whom US intelligence agencies believe to be drug smugglers***
  - **…*list of 12 provincial officials the US reportedly wants removed from office***

- ✓ **One shopkeeper said, "They were all stolen from offices inside the base by the Afghans working there," he said.**

**"Convenience Kills"**

# Identity Theft

- Michelle Brown, a victim of identity fraud from January 1998 - July 1999
  - Impersonator procured good and services worth over $50,000
  - Impersonator engaged in escalated level of crimes including drug trafficking
  - Damaged credit, erroneous arrest record, a warrant for arrest, and a prison record
- USA
  - 2003 to 2006 decreased total number of victims but an increase total value to US $56.6 billion in 2006
  - Average fraud, per person rose from $5,249 in 2003 to $6,383 in 2006
- Australia – Between $800 Million and $3.3 Billion in 2001
- United Kingdom – 2006 $3 Billion

# Lost, Stolen or Compromised PII

- Organization involved:  US Army Recruiting Command
- Date of incident:  February 17, 2007

- Brief description:
  - A Brigadier General's laptop was stolen from his hotel room
  - The PII data was not encrypted
  - The PII was in emails stored in exchange offline file on the laptop
  - PII is NCO Evaluation Report and Military Police Blotter Reports
  - Also, 300 Army recruiting prospects, some minors

- Describe actions taken:
  - Local police immediately notified
  - SJA responsible for notifying individuals whose information was compromised
  - NEC investigated what emails might have been on the laptop

# While Traveling

- Safety and security recommendations should be followed to protect laptops and safeguard sensitive data
- Use visual deterrents
- Avoid leaving unsecured laptops unattended
- Keep laptops inconspicuous
- Back-up valuable data on a scheduled basis
- Stay informed

# While Traveling

- Safeguard your data
- Carry laptop hard drive in jacket pocket
- Keep removable media separately in a backpack or briefcase
- Encrypt the data
- Check with IA personnel for latest advances prior to travel

# Reporting Lost, Stolen or Compromised PII or SI
# User Responsibility

a. Report immediately to your Information Assurance Security Officer (IASO) and/or local chain-of-command.

b. The Information Assurance Security Officer (IASO) and/or local chain-of-command will report it immediately to the RCERT- CONUS first, and then report it to the Fort Gordon NEC.

A Serious Incident Report (SIR) will be generated and reported per AR 190–45 under the following conditions:

(1) Access or compromise of classified, sensitive, or protected information (for example, Soldier identification information (SSN), medical condition or status, doctor-patient, or attorney-client privilege

(2) Compromise of systems that may risk safety, life, limb, or has the potential for catastrophic effects, or contain information for which the Army is attributable (for example, publicly accessible waterways navigational safety

# After Return from Travel

- Inform the approving authority that you have returned with the device and that it has been properly secured
- For Personally Identifiable Information, sign the data back in with the Security Officer or Supervisor
- If the device has been off the network more than 14 days or connected to another network, you must do the following:
  - IAM or IA personnel scan the mobile computing device for vulnerabilities and review
  - IAM or IA personnel scan the mobile computing device and data storage devices for viruses, worms, and trojans

## Remember these three important points!

- Users are the weakest link in MCD physical security
- Proper security and configuration of DAR protection on the device will prevent or hinder access and exploitation of the information
- Report Incidents

# Training video: Protecting Personally Identifiable Information

**Now view the training video on Protecting Personally Identifiable Information by clicking on the link below. Upon completion, you will be required to :**

1. **Print a certificate of completion**

2. **Provide this certificate to your unit or garrison Information Assurance Security Officer (IASO)**

https://iatraining.us.army.mil/_html/student.htm#reqtype=selcourse&pg=-1

# DAR Policy References

(https://ia.gordon.army.mil/refLib.asp)

- OMB Memo on PII
- DoDI 8500.2 Information Assurance Implementation
- AR 25-1, Army Knowledge Management and Information Technology
- AR 25-2, Information Assurance, numerous paragraphs
- Army CIO/G6 Memorandum: SUBJECT: Army Data-At-Rest (DAR) Protection Strategy, DTD: 28 SEP 2006
- Data-At-Rest (DAR) Protection – Mobile Devices using EFS Implementation (v1.0) BBP https://informationassurance.us.army.mil/bbp/BBP%20DAR%20VER%201%200.pdf
- “Road Warrior” Laptop Security BBP https://informationassurance.us.army.mil/bbp/BBP_Road_Warrior_VER_1_3.pdf
- AR 25-2, Section VIII Incident and Intrusion Reporting and https://www.rcert-c.army.mil/index.html
- AR 190–45, Law Enforcement Reporting: http://www.army.mil/usapa/epubs/pdf/r190_45.pdf

***QUESTIONS?***

***Please see your Unit or Garrison IA personnel***
***or contact the NEC Information Assurance Division at:***
**Usarmy.gordon.93-sig-bde.list.fg-nec-info-assurance-div@mail.mil**

**Data-At-Rest is Data-At-Risk!**